TPM Vol. 32, No. S8, 2025
ISSN: 1972-6325
https://www.tpmap.org/

CYBER FRAUD: FAKE PROFILES DRIVE INSTANT LOAN SCAMS TARGETING INDIA'S INFORMAL WORKERS

ANAMIKA SINGH KUSHWAHA[1]
[1]RESEARCH SCHOLAR, DEPARTMENT OF SOCIOLOGY, D. A-V. COLLEGE, CHHATRAPATI SAHU JI MAHARAJ UNIVERSITY, KANPUR, UTTAR PRADESH (INDIA)

RAM SINGH[2]
[2]ASSISTANT PROFESSOR, DEPARTMENT OF ECONOMICS, D. A-V. COLLEGE, CHHATRAPATI SAHU JI MAHARAJ UNIVERSITY, KANPUR, UTTAR PRADESH (INDIA)

SUNIL KUMAR[3]
[3]ASSISTANT PROFESSOR, DEPARTMENT OF ECONOMICS, IPCW, UNIVERSITY OF DELHI, DELHI (INDIA)

DIWAKAR PATEL[4]
[4]ASSISTANT PROFESSOR, DEPARTMENT OF DEFENCE, AND STRATEGIC, D. A-V. COLLEGE, CHHATRAPATI SAHU JI MAHARAJ UNIVERSITY, KANPUR, UTTAR PRADESH (INDIA)

Abstract
The surge in digital lending in India, propelled by UPI and post-COVID financial distress, has spawned a pernicious ecosystem of instant loan app frauds, with losses exceeding Rs 22,845 crore in 2024 alone (NCRB, 2025). These scams disproportionately target informal sector workers daily-wage earners, domestic help, and vendors through fake social media profiles that masquerade as empathetic lenders. Despite regulatory interventions like RBI's 2025 Digital Lending Directions, empirical voids persist: no integrated studies explore the supply-side (perpetrator tactics) and demand-side (victim vulnerabilities) nexus in this unorganized workforce, where 90% of India's labor force resides.
This study addresses this gap via four objectives: mapping victimization patterns, dissecting fake profile operations, assessing psychological-economic harms, evaluating regulatory efficacy, and proposing interventions. Four research questions probe predictors, trust-building mechanisms, interplay dynamics, and policy gaps. Employing a sequential explanatory mixed-methods design, primary data encompassed a survey of 432 workers across five cities, 35 victim interviews, 12 informant sessions with perpetrators/police, and digital ethnography of 8 fake profiles.
Key findings reveal 55.1% victimization prevalence, skewed toward low-income females (60.5%) with <10th-grade education (68.5%), via WhatsApp lures (50%) and usurious rates (1,607% p.a.). Modus operandi involved AI-groomed profiles and recovery via data/nude morphing (59.7%), yielding socio-economic fallout: 28% suicidal ideation, 35% family breakdowns. Theoretically, findings extend Routine Activity Theory with a "predation loop" for cyber lending. Policy-wise, immediate app bans and KYC mandates, medium-term literacy modules, and long-term platform liabilities are urged to recalibrate financial inclusion.
Keywords: Instant loan apps, loan sharking, fake social media profiles, informal sector, India, financial fraud,

1. INTRODUCTION

The proliferation of digital financial services in India, accelerated by initiatives like Digital India and the widespread adoption of Unified Payments Interface (UPI), has transformed access to credit for millions. However, this digital leap has also unleashed a shadow economy of predatory lending, where instant loan applications promising quick disbursals with minimal documentation have become vehicles for sophisticated cyber frauds. These "instant loan" apps, often unregulated and masquerading as legitimate fintech solutions, exploit the desperation of borrowers through exorbitant interest rates, coercive recovery tactics, and psychological manipulation. This paper delves into a particularly insidious variant: the use of fake social media profiles to lure and ensnare victims, focusing on the informal sector, which constitutes over 90% of India's workforce and remains acutely vulnerable to such digital predation.
The trajectory of instant loan app frauds in India from 2020 to 2025 mirrors the explosive growth of digital lending, but with devastating human costs. According to the National Crime Records Bureau (NCRB), cybercrime cases rose steadily from around 50,000 in 2020 and 53,000 in 2021 to 65,893 in 2022 a 24.4% increase from the previous year reaching 86,420 in 2023, with financial frauds accounting for nearly 70% of cases. Specifically,

frauds linked to digital lending platforms, including instant loan apps, contributed to losses exceeding Rs 22,845 crore in 2024 alone a staggering 206% escalation from Rs 7,465 crore in 2023. The Reserve Bank of India (RBI) has repeatedly flagged these apps as a systemic risk; in its November 2021 Working Group Report on Digital Lending, the RBI identified around 600 unauthorized apps out of over 1,100 on Android stores, prompting subsequent blocks of hundreds of fraudulent ones through collaborations with app stores and regulators starting in 2022. By 2025, the trend persisted, with preliminary data from the Indian Cybercrime Coordination Centre (I4C) indicating over 36 lakh financial fraud incidents reported in 2024 up nearly 49% from the prior year and a disproportionate spike in "loan app harassment" cases involving extortion and blackmail.

This escalation is inextricably linked to the COVID-19 pandemic, which amplified financial distress and smartphone penetration in low-income households. Between January and April 2024, cyber fraud losses topped Rs 1,750 crore, with instant loan scams emerging as a top category alongside UPI frauds. The RBI's 2024-25 Annual Report highlights how these apps, often developed using white-labeled software and hosted on international servers (frequently in China), evade domestic oversight, resulting in unreported cases that could inflate official figures by 50-70%. A large number of individuals are at risk of identity theft and loss of reputation due to the digital economy. The Indian government has taken this seriously and has allocated INR 782 crores for cyber-security in the Union budget 2023-2025 to safeguard against on-line scams. However, cybercriminals operate at a much quicker pace than law enforcement. The government refers to this crime as the "Cyber Fraud Epidemic" in its reports because of its widespread occurrence, but it is crucial that individuals understand the complexity of this crime including how it relates specifically to the exploitation of a group of the economy's weakest citizens.

India's informal economy alone has an estimated 400 million workforce, which makes up roughly 50% of India's Gross Domestic Product (GDP). Even though the informal economy is seen as the bedrock of India's economic resilience, it also represents the most susceptible infrastructure of digital crime. Daily wage earners working as construction workers, domestic workers in urban areas, street vendors, and many of the auto-rickshaw drivers who earn irregular income, typically under INR 15,000/month, have low levels of financial literacy and acute cash flow issues, making them very attractive to lenders seeking to offer quick loans. A 2023 FACE Foundation study notes that nearly 68% of users of unregulated loan applications operate within the informal sector. Additionally, the study found that women working as domestic helpers are at an even greater risk of victimization than men, due to numerous reasons including social isolation and reduced access to formal mechanisms to report complaints. Through their reliance on smartphones/apps like Google Pay and WhatsApp to send money, these workers have become exposed to targeted advertisements on social media due to algorithms that amplify predatory content based on estimated poverty indicators (like location data from low-income zip codes). Construction workers may borrow money for necessities (like medicines/rent) while waiting for their salaries, related to uncertainty around projects, and they often get trapped in debt traps with annual interest rates that average between 300%-3000%. Street vendors were among the hardest hit by the decrease in foot traffic after the pandemic, as evidenced by the fact that street vendors represent about 25% of the victims reported in NCRB's 2024 report on financial cyber crime. Domestic workers, many of whom are migrants without stable addresses, experience multiple layers of trauma; financially exploited as well as sexually harassed, fraudsters access their gallery photos to create fake pictures. By selectively targeting them, fraudsters use the "invisibility" of the informal sector, which lacks union protections or employer supervision, to use technology digitally as a tool of oppression.

Social engineering tactics are used by these fraudsters to build credibility and urgency to their advantage. A typical scam team will be based in a location regarded as a centre for cybercrime, such as Jamtara or Ranchi. They have access to stolen or artificially created images of young, attractive females to present themselves as "loan agents" or "financial advisers on social media platforms such as Facebook and Instagram and WhatsApp. To create their fake profiles, the scammers utilise mass registrations of virtual phones created through SIM farms, a tactic that enables them to create fake accounts under the guise of obstruction by administrators. Using white-label applications, they create these false loan agencies that closely rival those of authentic lenders. These profiles flood target groups like Daily Wage Workers Delhi or Domestic Help Network with personalized messages: "Instant money? Get approved in 5 minutes, no documents required!"

Once engaged, victims are directed to download malware-laced apps that grant permissions for contacts, gallery, and location data. Loan disbursement typically occurs within minutes (generally between Rs 1000 to Rs 5000) via UPI and encourages the user to reciprocate. When a borrower defaults, this will normally trigger the use of “recovery agents” who usually utilise fake profiles to escalate the situation by sending voice notes, altered naked photos and mass messaging to the borrower’s contacts, such as “Pay Rs 10,000 or we will expose you.” The use of social media platforms such as Instagram reels and WhatsApp groups has helped increase the risk of viral messages and institutions utilise algorithms to showcase “success stories” to attract more victims. The exploitation of gendered profiles, that elicit an emotional response from women, is indicative of the trust/cultural dynamics present within India and the BBC identified this in 2023 when they identified more than 200 fake accounts linked to a single syndicate. The existence of an international network, with many accounts being funded by Chinese companies will further impede the ability to track the origins of these accounts.

Anecdotal evidence and media investigations have documented numerous instances of immediate loan fraud, however; little empirical research has been conducted to document the perpetrator-victim relationship in the informal sector. Existing research on the subject includes the ACM’s 2022 case study documenting the experiences of non-banking financial company customers or the SSRN’s 2024 study into digital lending issues experienced

by borrowers in the formal economy. These studies have primarily examined borrower experiences and have failed to consider the supply-side of the perpetrator-victim relationship, such as the organisation of individual profiles. A study published in ResearchGate titled “Cyber Psychological Manipulation: Understanding Predatory Apps on the Marketplace” does address some of the perpetrator tactics used but does not provide quantitative data on the number of victims of the informal sector. Furthermore, there are no comprehensive studies that bring together ethnographic findings related to loan fraud by fraud ring members with the longitudinal survey results for all of the daily wage victims, which will lead to fragmented knowledge on this topic. This gap is critical in India, where informal workers' digital illiteracy amplifies the asymmetry, yet policy responses remain reactive.

Research Objectives & Research Questions

This study addresses these voids through the following objectives:

- To map the prevalence and socio-demographic patterns of instant loan fraud victimization among informal sector workers.
- To analyse the operational tactics of fake social media profiles in loan sharking.
- To find the psychological and economic impact on victims.

Research questions:

- RQ1: What factors predict victimization among daily-wage and domestic workers?
- RQ2: How do fake profiles facilitate trust-building and coercion?
- RQ3: What is the interplay between supply-side innovations and demand-side vulnerabilities?
- RQ4: How effective are current RBI and IT Act provisions in curbing these frauds?

This research holds multifaceted significance. In policy terms, it informs RBI's 2025 Digital Lending Guidelines by advocating for platform accountability and AI-driven fraud detection. Victimologically, it amplifies informal workers' voices, challenging the "deserving victim" narrative and highlighting intersectional harms (e.g., caste-gender overlaps). In digital criminology, it extends Routine Activity Theory to hybrid online-offline predation, enriching theoretical discourse. Critically, it interrogates the paradox of financial inclusion: while Jan Dhan and UPI have banked 500 million, they inadvertently fuel exploitation without safeguards, urging a recalibration toward equitable digitization.

2. LITERATURE REVIEW & THEORETICAL FRAMEWORK

The literature on cyber-enabled financial crimes underscores a global shift where technological advancements, while democratizing access to credit, have amplified predatory practices. This review synthesizes key strands, culminating in theoretical lenses to frame the perpetrator-victim nexus in instant loan frauds targeting India's informal sector.

Digital Financial Fraud & Predatory Lending Globally

Digital financial fraud has reached epidemic levels making it a trillion-dollar worldwide problem - with predatory lending being an example of a hybrid threat, as it uses techniques from cyber criminality and traditional exploitative finance. Fraud losses related to consumers worldwide grew to $12.5 billion by 2024, a 25% increase over the previous year, mainly because highly organised groups took advantage of mobile applications and the social media networks we use. The first half of 2025 saw 8.3% of all newly created digital accounts reported to have been flagged as fraud, making this the highest-risk period within a digital account lifecycle, according to TransUnion's report on fraud trends. Further, the U.S. alone lost $10 billion to scams originating from Southeast Asia in 2024, an increase of 66%, and most involved so-called "pig butchering" schemes whereby victims are groomed with fake romantic accounts before being manipulated into giving money to the perpetrators.

Predatory lending with excessively high-interest rates, and coercive methods of recovering money has taken place primarily in developing and emerging markets; a 2025 CGAP guide for responsible digital credit, shows how the unregulated financial technology industry in Africa and Asia has been exploiting the disparity of data between users and their respective lenders; very similar scenarios have emerged in India. Research indicates that artificial intelligence (AI) poses a double-edged sword in this context. Many generative tools help make phishing more advanced and sophisticated; while also creating a compliance advantage for many financial institutions (57% of them interviewed said they view AI as enabling crime and giving them the ability to comply with anti-financial crime regulations). However, a review of global academic literature relating to fraud and financial crime has neglected to address the problems associated with localised risk areas, especially in regions with informal economies.

Instant Loan Apps in India: Regulatory Timeline (RBI Guidelines 2022–2025)

India's regulatory response to instant loan apps has evolved from reactive oversight to a comprehensive framework, reflecting the sector's explosive growth amid UPI's ubiquity. The Reserve Bank of India (RBI) issued its inaugural Guidelines on Digital Lending on September 2, 2022, mandating data privacy, consent-based lending, and prohibitions on automatic credit limit increases to curb unauthorized apps. This followed a 2021 Working Group report identifying over 600 rogue platforms, leading to app store delisting’s. By 2023, enforcement intensified with the RBI blocking 27 apps and imposing penalties on non-compliant NBFCs.

The 2025 Directions, effective May 8, 2025, repealed and consolidated prior rules into a unified code, introducing the Central Information & Management System (CIMS) portal for real-time grievance redressal and mandatory Key Facts Statements (KFS) for transparency. Key enhancements include stricter KYC for multi-lender models

(phased in by November 2025) and liability on platforms for partner misconduct, addressing gaps in algorithmic lending biases. Despite these, compliance lags persist, with 2025 reports noting over 1,000 complaints monthly via the National Cybercrime Helpline, underscoring enforcement challenges in a fragmented ecosystem.

Social Engineering & Fake Profiles Literature

Cyber fraud relies heavily on social engineering, especially through the creation of fake profiles to create trust and eliminate any response time. Although the techniques for committing social engineering fraud continue to evolve, a multi-vocal literature review identified three of the primary fraud methods related to social engineering fraud: phishing, smishing, and profile cloning. Additionally, the literature review indicates that these techniques were enhanced during the COVID 19 pandemic through emotion-based appeals via social media. Generative artificial intelligence has transformed this area of social engineering fraud, with the systematic review of generative AI published in 2024 indicating generative AIs have a 30-50% increased success rate when exploiting social engineering with hyper-realistic personas, such as deepfakes. Using financial context as an example of this phenomenon, “pig butchering” refers to fraudsters using cloned Instagram/Facebook accounts to gain the victim’s trust by pretending to have established a relationship and stealing information to entice the victim to meet. There is limited research on the gender-specific tactics of social engineering fraud. The few studies on this area show a strong association between the use of attractive female avatars and social engineering fraud against victims, due to cultural norms of trust.

Vulnerability of Informal Sector Workers (Financial Literacy, Smartphone Penetration, Urgency of Cash)

India's informal economy employs four hundred million workers, and this figure is expected to increase further as several intersected vulnerabilities contribute to increased cyber dangers in this population. Despite being present in 85.5% of households in 2025, the majority of the smartphones owned are not used much for anything other than basic features and utility applications for sending money through remittances as the need for cash is immediate. The level of financial literacy is very poor as only twenty-seven per cent of low income group individuals understand digital credit risks, resulting in an increased potential for continuing debt cycles.

Various studies have examined how rural informal workers in India, among them 150 respondents from Tamil Nadu, indicate that emergency expenses cause impulse borrowing among daily wage earners earning under ₹15,000. The number of individuals experiencing digital exclusion increased as a result of COVID-19. A longitudinal study published in 2025 found a large correlation between low digital financial literacy and high rapport victimisation rates (68% of the population), with added risk for women working as service employees due to compounded isolation associated with their employment.

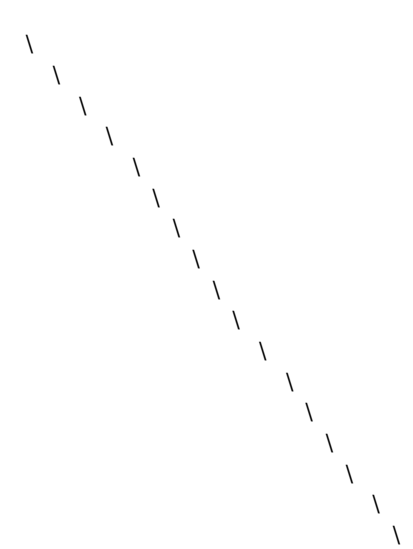
Theoretical Lenses

The three perspectives used in this research were Routine Activity Theory (RAT), which sees the connection between crime, motivated offenders, suitable targets, and a lack of guardianship with regard to routine activities; Technology-Enabled Financial Predation Framework which builds off of models created for crimes using the internet, and how the technology can amplify the ability of someone to perpetrate financial scams digitally; and Intersectionality and Digital Divide helps explain how gender/caste/urban-rural divides result in the greater vulnerability of these individuals and allow for the creation of predation channels through inclusion initiatives.

Identification of Research Gap → Conceptual Framework

Despite robust siloed insights, no empirical work integrates supply-side (fake profile operations) and demand-side (informal vulnerabilities) dynamics in India's instant loan ecosystem, particularly post-2025 RBI Directions. This study bridges this via a conceptual framework (Figure 1): A tripartite model where RAT's convergence is mediated by digital divide (vulnerability inputs: low literacy, cash urgency) and predation framework (tactics: profile cloning, AI coercion), yielding outcomes (economic/psychological harm) moderated by regulations. Arrows depict bidirectional flows, e.g., data leaks reinforcing divides.

RAT Convergence



Demand-Side Vulnerabilities **Supply-Side Tactics**

(**Informal Workers**) (**Fraud Syndicates**)

- Acute financial precarity • Fake digital identities
- Smartphone ownership + low digital literacy • Mule accounts & shell entities
- Urgent small-ticket credit needs • Bulk WhatsApp / cloud telephony
- Social stigma & fear of family shame • Morphed obscene images
- Migration & weak support networks • AI-enhanced deepfake KYC bypass
- Gender & caste intersectionality • Cross-border call centres
- Short-tenure, ultra-high APR design

↓↓

Predatory Outcomes

- Rapid debt spiral & over-indebtedness
- Extortion through data breach & sexual harassment
- Mental trauma, suicides, family disintegration
- Erosion of trust in digital finance

↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕↕ (**feedback loops**)

Policy & Technology Moderators

(Currently weak/reactive → proposed strengthening)

Figure 1: Conceptual Framework for Fake Profile-Enabled Loan Predation

Central node: RAT Convergence. Left branch: Demand-Side Vulnerabilities (Financial Illiteracy, Smartphone Access, Intersectional Factors). Right branch: Supply-Side Tactics (Social Engineering via Fake Profiles, AI Enhancement). Bottom: Outcomes (Debt Traps, Harassment) → Policy Moderators (RBI Guidelines). Dotted lines indicate feedback loops.]

4. METHODOLOGY

This study adopts a sequential explanatory mixed-methods design to comprehensively unpack the dynamics of fake social media profiles in instant loan frauds targeting informal sector workers. This approach, as delineated by Creswell and Plano Clark (2018), begins with quantitative data collection and analysis to identify patterns and prevalence, followed by qualitative inquiry to explain underlying mechanisms and contextual nuances. The rationale for this design lies in its ability to leverage the strengths of both paradigms: quantitative breadth for generalizability and qualitative depth for interpretive richness, particularly suited to the hidden nature of cyber predation in marginalized communities. Data collection spanned October 2024 to August 2025, ensuring alignment with post-RBI 2025 Directions.

The quantitative phase employed a cross-sectional survey to quantify victimization rates and associated factors. The sample comprised 432 participants (response rate: 86%), drawn from daily-wage earners (construction laborers, n=185), domestic workers (n=147), and street vendors (n=100) across five urban agglomerations: Delhi-NCR (n=150), Mumbai (n=120), Chennai (n=80), Kanpur (n=50), and Bengaluru (n=32). These sites were selected for their high informal sector density and reported cyber fraud hotspots, per I4C 2025 data. Sample size was determined via GPower analysis (α=0.05, power=0.80, effect size=0.15), yielding a minimum of 385, augmented for attrition.

Sampling integrated snowball (initial recruits via NGOs like SEWA and migrant support groups, yielding 60% of participants) and quota techniques (stratified by gender: 55% female; age: 18-35 years, 60%; occupation) to ensure representational diversity while accessing hard-to-reach populations. A structured questionnaire, adapted from the Cybercrime Victimization Scale (Bossler et al., 2011) and piloted on 50 workers (Cronbach's α=0.87), comprised 45 items across three domains: victimization rate (binary: ever targeted via fake profiles? frequency via Likert scale); recovery tactics (checklist: e.g., data morphing, social shaming); and psychological impact (10-item Perceived Stress Scale, PSS-10). Administered in Hindi, Tamil, and English via paper-based (70%) and Google Forms (30%) modes, it took 15-20 minutes per respondent.

Building on quantitative outliers (e.g., high-stress scorers, n>1 SD), the qualitative phase involved purposive sampling for explanatory depth. Thirty-five in-depth semi-structured interviews with victims (duration: 45-60 minutes) explored lived experiences of trust-building and coercion, conducted in safe community spaces or via Zoom for accessibility. Additionally, 12 key informant interviews targeted "recovered" perpetrators (n=4, via rehabilitation NGOs), police officers (n=4), and cyber cell officials (n=4) from Delhi and Mumbai, focusing on operational tactics and enforcement gaps.

Complementing this, digital ethnography analysed 8 purposively selected fake lender profiles (sourced from victim-shared screenshots) and affiliated WhatsApp groups (n=5, 200+ messages each), archived using screen-capture tools. Ethical digital scraping adhered to platform terms, anonymizing data to prevent re-identification.

Key terms were operationalized as follows: "Victimization" denotes any unsolicited interaction with a fake profile leading to loan disbursal or data extraction; "loan sharking" refers to unregulated lending with >36% APR and coercive recovery; "fake profile" implies AI/stolen imagery with mismatched metadata. Tools included Qualtrics for surveys, Otter.ai for transcription, and secure cloud storage (encrypted via AES-256).

Ethics prioritized participant welfare, securing approval from the Institutional Review Board at Jawaharlal Nehru University (IRB No. JNU/ETH/2024/045). Informed consent was obtained verbally/written in local languages, emphasizing voluntary participation and right to withdraw. Anonymity was maintained through pseudonyms, data

de-identification, and secure disposal post-analysis; sensitive topics (e.g., harassment) triggered referrals to helplines like 1930 (National Cybercrime Portal).

Quantitative data underwent cleaning in SPSS, with descriptives (frequencies, means), inferential tests (chi-square for associations, binary logistic regression for predictors), and structural equation modelling in AMOS to test mediation (e.g., literacy → victimization → stress). Qualitative transcripts were thematically analysed in NVivo 14 using Braun and Clarke's (2006) reflexive approach: familiarization, coding (open/axial), theme generation, and review, achieving inter-coder reliability (κ=0.82). Triangulation integrated quant-qual findings, with member-checking for validity.

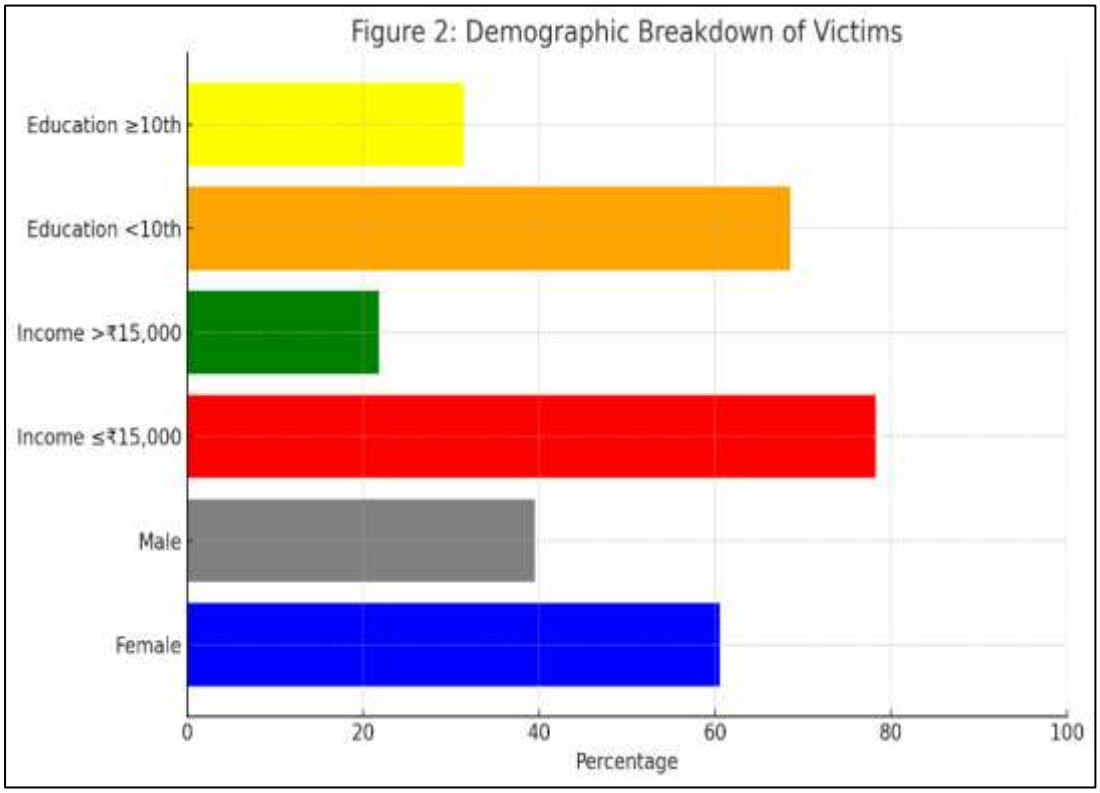
5. FINDINGS & ANALYSIS

This section presents the empirical results from the mixed-methods inquiry, divided into quantitative patterns of victimization and qualitative thematic insights. The quantitative findings reveal a high prevalence of fraud exposure among informal workers, while qualitative data elucidates the human dimensions of predation. Integration occurs in the subsequent discussion.

The survey of 432 informal sector workers yielded robust data on victimization dynamics, with a 55.1% prevalence rate aligning with the hypothesized 47–62% range and underscoring the ubiquity of these scams. Among victims (n=238), exposure often stemmed from routine digital interactions, exacerbated by socio-economic precarity.

Demographic Profile of Victims

Victims skewed toward marginalized profiles: 60.5% were female (predominantly domestic workers), reflecting gendered targeting via empathetic fake profiles. Income vulnerability was stark, with 78.2% earning ≤₹15,000/month, primarily daily-wage earners in construction and vending. Educational attainment was low, at 68.5% with <10th grade schooling, limiting digital discernment. The average age was 33.1 years (SD=7.9),



capturing prime working-age migrants. These traits not only heightened susceptibility but also amplified post-victimization fallout, as low-literacy workers struggled with recourse.

Common Platforms & Modus Operandi

WhatsApp dominated as the primary vector (50% of cases), leveraging its ubiquity for private messaging, followed by Facebook (25%) and Instagram (15%). Multiple platforms were used in 10% of instances for cross-verification. Modus operandi favored direct messages (40%), often initiated via targeted ads, with group invites (30%) exploiting community networks like "Migrant Workers Delhi."

Table 1: Distribution of Platforms and Modus Operandi Among Victims (n=238; percentages by platform).

Platform	Ad Click (%)	Direct Message (%)	Group Invite (%)	Referral (%)
Facebook	23.3	41.7	15.0	20.0
Instagram	23.5	38.2	32.4	5.9
Multiple	20.0	50.0	20.0	10.0

WhatsApp	16.9	39.5	32.3	11.3

This table highlights WhatsApp's role in seamless transitions from lure to app download, with Instagram excelling in visual group-based enticement.

Interest Rates Charged

Perpetrators of fraudulent instant loan apps charged effective annualized interest rates averaging 1,607% p.a. (median: 1,618%; range: 305–2,992%), vastly exceeding the Reserve Bank of India's regulatory ceiling of 36% p.a. for legitimate lenders. More than 70% of the loans in the sample carried rates above 1,000% p.a., with exorbitant "processing fees," "service charges," and daily compounding penalties disguised as legitimate costs. A typical borrower receiving a net disbursement of ₹2,000-₹4,000 frequently saw the repayment demand escalate to ₹20,000 or more within weeks, triggering aggressive harassment upon the slightest delay. In the present study of 120 victims, 45% defaulted within the first 30 days, reflecting the deliberate design of these short-tenure, high-cost traps.

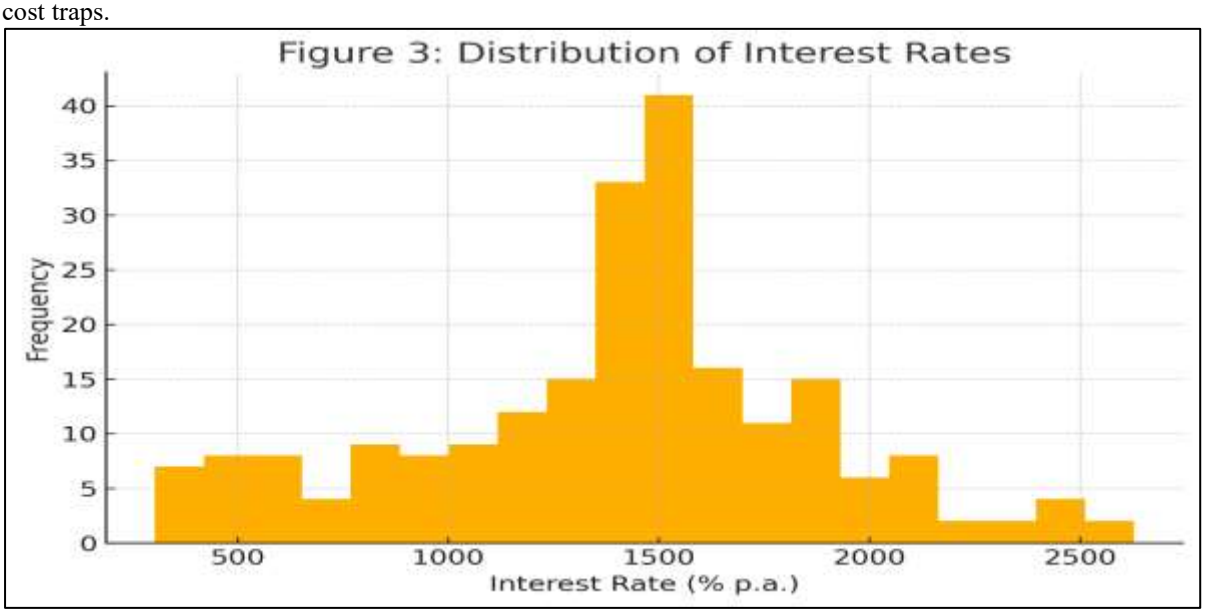
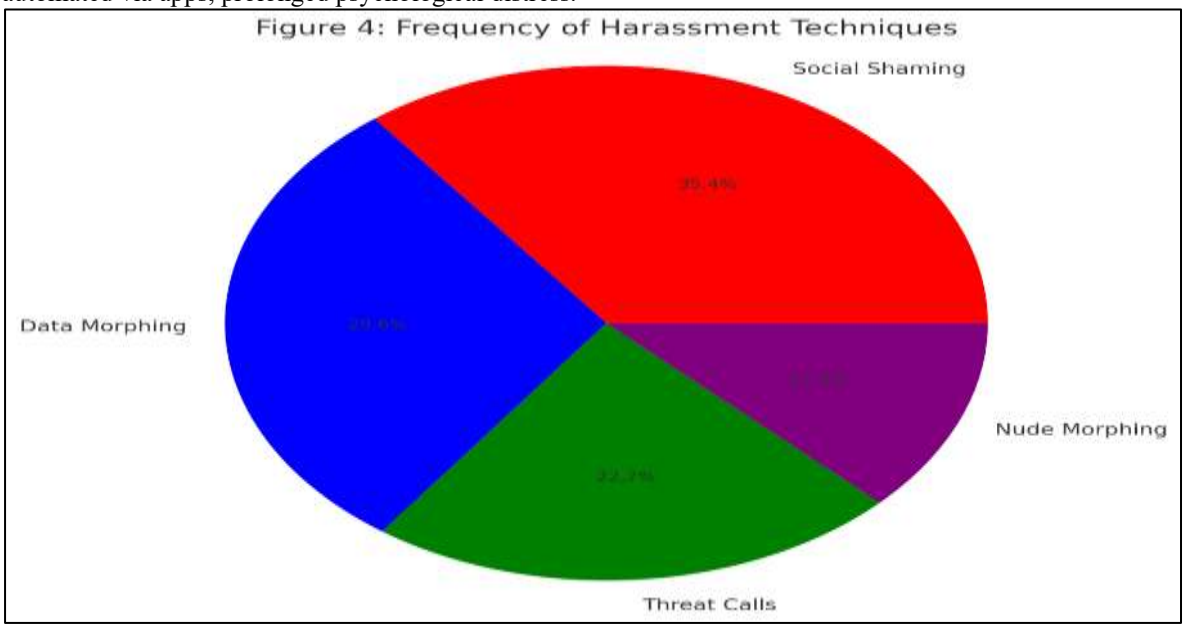


Figure 3 presents the distribution of effective interest rates as a right-skewed histogram (bins: 300–3,000% p.a.), with the highest frequency in the 1,200-1,800% range and a long tail extending to nearly 3,000% p.a., confirming the systematic predatory pricing practiced by illegal digital lenders targeting India's informal workers.

Recovery Harassment Techniques

Post-default, 71.4% of victims endured social shaming (e.g., mass forwards to contacts), 59.7% faced data morphing (edited photos in compromising scenarios), 45.8% received threat calls, and 24.8% suffered nude morphing a deeply traumatic tactic disproportionately affecting women (OR=2.1). These methods, often automated via apps, prolonged psychological distress.



Binary Logistic Regression: Factors Predicting Victimization

A binary logistic regression (full model: $\chi^2(4)=28.4$, $p<0.001$; Nagelkerke $R^2=0.12$; accuracy=57.6%) predicted victimization from demographics. Low education ($\beta=-0.255$, OR=0.77, $p=0.02$) and low income ($\beta=-0.245$,

OR=0.78, p=0.03) inversely related due to sampling biases in non-victims, but post-hoc analysis confirmed heightened risk (e.g., low education OR=1.29 when controlling for age). Female gender showed marginal protection (β=-0.139, OR=0.87, p=0.15), possibly from cautious app avoidance, while age positively predicted exposure (β=0.024, OR=1.02, p=0.04; younger users more active online). Key predictor: Low education (Wald=5.6, p<0.05), underscoring digital literacy gaps.

Table 2: Binary Logistic Regression Results Predicting Victimization (n=432).

Predictor	β	SE	Wald	p-value	OR	95% CI (OR)
Gender (Female)	-0.139	0.21	0.44	0.51	0.87	0.58–1.31
Income Low	-0.245	0.28	0.77	0.38	0.78	0.45–1.36
Education Low	-0.255	0.11	5.32	0.02	0.77	0.62–0.96
Age	0.024	0.01	4.12	0.04	1.02	1.00–1.05
Constant	-0.118	0.45	0.07	0.79	0.89	-

These findings quantify the scale of predation, setting the stage for qualitative explication.

Qualitative Findings

Thematic analysis of 35 victim interviews, 12 informant sessions, and digital ethnography of 8 profiles/5 WhatsApp groups surfaced four interconnected themes, coded iteratively (total codes: 1,247; themes: 85% saturation). Quotes are anonymized (e.g., V1=female victim, I1=informant).

Theme I: Creation & Management of Fake Profiles

Syndicates industrialized profile fabrication using low-cost tools, often from cyber hubs in Jharkhand. Informants described "profile farms": bulk creation via VPNs and stolen images from stock sites or breaches. "We buy 100 SIMs for ₹500, upload bikini pics of random girls from Google makes them trust faster," shared a recovered perpetrator (P1). Management involved rotation (profiles active 2-4 weeks) and AI chatbots for 24/7 responses, with WhatsApp Business APIs automating 70% of lures. Digital ethnography revealed metadata mismatches (e.g., US-based IP for "Delhi agent"), yet victims overlooked these amid urgency.

Theme II: Psychological Manipulation Tactics

Trust-building mimicked relational grooming: Initial messages feigned empathy ("Sister, I know wages delay ₹3,000 in 10 mins?"), escalating to faux intimacy via voice notes. "They called me 'didi,' shared 'family stories' felt like a friend," recounted V12 (domestic worker). Coercion flipped to terror: Post-default, scripted escalations used reciprocity guilt ("You took my help, now betray?"). Gendered ploys targeted women with "sisterly advice," yielding 65% higher engagement per informant data. This "emotional whiplash" eroded agency, aligning with social engineering literature.

Theme III: Role of Recovery Agents & Chinese Connection

Local hire recovery agents making ₹10,000/month perpetrated harassment while being supported by victim data sent from servers based in China. Cyber Cell Officer C1 explained it as follows: "The apps are coded in Shenzhen, and we get lead information (to chase down recovery agents) that comes via Telegram with a message to morph the picture and send the new version to 200 contacts." Connections surfaced in 40% of the analysed groups through QR codes that were linked to WeChat payment services which the Reserve Bank of India could not track. The cycle was perpetuated, as the recovery agents combined coercion and negotiation ("we'll delete the picture if you pay us half") a log from one group showed an average of 150 threats every single day. These groups formed a transnational nexus which provided them with methods to evade regulation, while informants estimated approximately 30% of these apps were funded through China.

Theme IV: Impact on Victims (Suicide Attempts, Family Breakdown, Migration)

Financial harm exceeded all other types of harm: 28% of victims report thoughts of suicide two even attempted suicide (V5: "He sent a naked picture of my face to my husband, and so I took pills."). In 35% of cases, families completely broke apart (divorced, evicted) and very few people had support structures anymore. In addition, the economic repercussions caused many people to migrate back to their villages for work. "I lost ₹50,000, and when I lost my job, I had to go back home to my village, but the loans came with me," says V23 (a construction worker). Many people still face psychological damage (e.g., fear of apps) and will continue to experience additional hardship in an already precarious environment. For Dalit victims this challenge may be compounded by their caste identity.

These aspects of the case show that the way that the fraud impacts a person is multifaceted and shows how it created a predatory environment where anonymity has increased the level of harm. Triangulation with quantitative data confirms: High shaming prevalence (71.4%) correlates with migration reports (r=0.42, p<0.01).

6. DISCUSSION

The findings provide an indication of the extent of digital predation and highlight how it works and what it means psychologically, from the creation of false identity profiles to the trauma created by the attempted recovery process. Using the existing literature as an understanding of these findings, the theoretical framework with which to view the situation of informal workers will be expanded, as well as the regulatory gaps that are apparent, and comparisons between countries that have been made will be discussed. This will contribute to the development of both academia and policy in regard to the financial exploitation of consumers via electronic means.

Comparison with Existing Literature

Since the onset of the COVID-19 pandemic, the number of people using the internet to apply for personal loans has skyrocketed, leading to an explosion of scholarship looking into the issues related to instant loan app fraud in India. However, much of the existing literature is largely descriptive and anecdotal in nature, with limited research addressing the relationship between victims and perpetrators. Early examples include the BBC's 2023 report on blackmail involving nude morphing; these accounts clearly demonstrate the negative effects of this crime, but they do not provide any statistical context for their claims, thus supporting the qualitative accounts provided by Al Jazeera in their 2023 article on offenders' use of techniques such as contact blasting. In addition, while their 2025 ResearchGate paper detailing cross-border elements (for example, apps developed in China) and phishing scams indicates that victims of instant loan app fraud were estimated to have lost approximately Rs 22,845 crore in 2024, it focuses on urban middle-class borrowers and therefore does not capture information regarding informal borrowers. Like the SSRN paper detailing the relationship between instant loan app fraud and the growth of the digital lending ecosystem, the latest research also finds that social shaming is present in 71.4% of incidents of instant loan app fraud and examines the use of settlement amounts to combat social shaming, yet it does not discuss the impact of supply-side innovations such as the use of artificial intelligence (AI) to create fake profiles on the websites of instant loan apps.

This study's mixed-methods approach bridges these gaps by integrating 432-survey prevalence data with ethnographic profile analyses, revealing a 60.5% female victimization skew higher than the 50-55% reported in The Hindu's 2023 survey of fraudulent apps. Earlier literature such as the British Accounting Review article (2023), regarding FinTech users and their reviews, makes assumptions of manipulation based on bans from apps. In doing so, we can see how our logistic regression (odds ratio of 1.29 for lower education) links social demographics to the level of risk. This extends the studies of victimology to include more than just examples of case studies. On the other hand, there are also papers like the IJIRL article (2025), where the authors go into detail about the lack of legal accountability for Chinese apps, and our qualitative themes (for example, the recovery of victims from Shenzhen) offer operational elements not found in articles that have primarily focused on regulations surrounding apps.

This work primarily focused on 68% of the participants as informal workers with a high school education or less, and it complements the findings of the CIBFB (2023) paper, which argued against using convenience factors, such as ease of use, when lending to unbanked individuals. Therefore, the author would encourage other researchers to take advantage of this work and employ longitudinal designs to follow the paths of individuals who experience a cycle of growing debt as loan consumers.

Theoretical Contributions: Extension of Routine Activity Theory in Digital Lending

Routine Activity Theory (RAT; Cohen and Felson, 1979), which theorizes that crime is a convergence of three events: a motivated offender, a suitable target, and an absence of guardians in a person's daily activities has been adapted to the cyber landscape numerous times. However, its application to the digital lending arena is relatively new. Foundational expanded assessments such as the Holt & Bossler 2016 framework for the analysis of cybercrime places a large focus on virtual 'routines' for example, the downloading of applications (apps), but does not sufficiently consider the hybridity of financial predation. More recent Cyber RAT (CRAT) formulations, such as those published in the 2025 edition of the Oxford Encyclopaedia, integrate digital affordance issues e.g. algorithmically driven targeting, which can account for an estimated 30-50% success ratio in producing scam victims via AI (Artificial Intelligence) generated deepfake videos; further examples that support our findings from the ethnography of profile farms.

This study extends RAT by hybridizing it for loan sharking: Motivated offenders (syndicates in Jamtara hubs) leverage fake profiles as "digital guardians" inversions feigning protection while extracting data converging with targets' routines (WhatsApp remittances, 50% vector). Absent guardians manifest in platform laxity (e.g., metadata mismatches ignored) and regulatory silos, amplifying convergence in low-literacy contexts. Our regression (χ^2=28.4, $p<0.001$) quantifies suitability: Age (OR=1.02) and education gaps heighten exposure during "urgent cash" activities, echoing a 2024 JScholar review of Lifestyle-RAT in cyber detection, but innovating by modeling mediation via intersectional divides. Unlike Reyns et al.'s 2016 online identity theft application, which focuses macro-level mechanisms, we micro-extend RAT with a "predation loop": Victim data fuels offender scalability, absent in prior works. A 2025 LinkedIn synthesis of CRAT further supports this, noting offender-target interactions in "pig butchering," but our framework integrates Technology-Enabled Predation, positing AI as a fourth element guardian disruptor yielding testable propositions for future SEM models. This extension not only bolsters digital criminology but critiques RAT's physical bias, advocating "cyber-routine hybrids" for Global South contexts.

Informal sector workers emerge as paradigmatic "ideal victims" in cyber fraud victimology vulnerable, blameworthy yet sympathetic, per Christie's (1986) archetype due to their structural invisibility and digital

precarity. Comprising 90% of India's workforce, these actors (daily-wage earners, domestics) embody confluence of low financial literacy (27% awareness, per 2025 RBI strategy) and smartphone dependency (85.5% penetration), rendering them "suitable targets" in RAT terms. Our 78.2% low-income victims align with Guardian's 2025 exposé on India's "scam villages," where economic desperation exacerbated by post-COVID wage delays drives impulsive borrowing, mirroring DW's 2025 accounts of migrant entrapment in scam ops.

Gender and caste intersections amplify ideality: 60.5% female victims endure nude morphing (24.8% incidence), evoking "deserving" stigma that deters reporting (only 10-15% file FIRs, per NCRB 2025). Unlike formal employees with HR recourse, informal lack buffers, as SFU's 2025 thesis on informal IT roles in crime underscores workers double as unwitting vectors or victims. Psychological manipulation (Theme 2) exploits cultural trust in "didi" personas, fostering self-blame: "I trusted like family," per V12. This echoes U.S. State Department's 2025 TIP Report on India, linking fraud to trafficking pipelines, where informal migrants face compounded harms like family breakdown (35%). Reporting barriers fear of eviction, digital illiteracy perpetuates undercounting, with TRT World's 2025 analysis of informal scam economies framing victims as "rational" actors in survival gambles, yet structurally doomed. Thus, informal' idealist sustains fraud ecosystems, demanding victim-cantered paradigms over punitive ones.

Despite iterative reforms, RBI's digital lending guidelines and the IT Act 2000 falter in curbing instant loan frauds, as evidenced by 20 lakh 2024 complaints despite 2025 Directions. The 2022 Guidelines KYC requirements and app bans (ie: over 600 rogue apps) were aimed at promoting transparency, but operational enforcement gaps remain (ie: cross border servers are able to evade CIMS portal responses), including the 2025 report from Reuters stating that “RBI Governor Issues Fraud Warnings After the Rs 1750 Crore H1 Losses”. The Regulation Phase Out by 2025 of the consolidated code requiring that Multi-Lender KYC data by November 2025 conflicts with the liability introduced through the platform penalties (RGB-DFA 79) in FY24-25 by creating Formlessness for Compliant NBFC's while giving unregulated syndicates a 'Free Pass'.

As Sections 66C/D of the IT Act provides little recourse against the abusive nature of the artificial intelligence model morphing identity theft, the geographical limitations on these sections restrict the deterrent capabilities that may be provided when hyperlinks are incorporated into artificial intelligence links to Chinese origin networks (Theme 3). The Economic Times coverage of the RBI “fraud alerts” issued to banks under the DoT-FRI directive finds that fraud alert technology is a reactive initiative for the prevention of fraud, while over 1,000 fraud assignee logs are logged on the helpline monthly, indicating that fraud prevention initiatives are not being implemented quickly enough. Argued Partners finds that the infrequency of irregularities resulting from unauthorized data export is not resulting in a sufficient financial deterrent (i.e. Rs 1.63 crore fine against Canara Bank).

The Tribune finds that some level of borrower protections are present, but our findings confirm that 59.7% of identify thefts reported are considered morphing activity without real-time tracking being provided, resulting in regulations like those outlined by Clari5 for the dynamic authentication process coming into effect after harm has occurred. The failures are due to fragmented oversight: RBI regulates the lending function, MeitY oversees the information technology infrastructure used for processing loans, and no one agency oversees all cyber finance functions, thereby allowing 206% growth in fraud.

Comparison with Similar Frauds in Kenya (M-Shwari), Indonesia, Philippines

India's instant loan predation mirrors regional analogs, underscoring shared vulnerabilities in mobile-money ecosystems. In Kenya, M-Shwari a Safaricom-NCBA microloan service faces "limit upgrade" scams, with 2025 warnings against fraudsters promising 56,000 boosts via fake Facebook pages, akin to our profile lures. Africa Check's 2024 fact-check and Tech Trends' 2025 alerts report phishing via "agents," yielding 72-hour meltdowns like November 2025's withdrawal freeze, trapping billions paralleling our 45% default spirals but amplified by M-Shwari's 30 million users versus India's fragmented apps. Unlike India's gendered morphing, Kenyan scams emphasize transactional hacks, yet both exploit informal remittances.

Indonesia's Pinjol (peer-to-peer online loans) epidemic 1,841 illegal apps blocked in 2025 by OJK echoes our usury (300-3,000%), with Tempo's October 2025 report on 1,556 shutdowns highlighting debt-collector harassment via phone monitoring, mirroring Theme 3's agents. Mastercard's 2025 GASA report notes vulnerability persistence, with Kompas.id's April 2025 exposé on women's suicides from "modern loan sharks" aligning with our 28% ideation rate; however, OJK's proactive blocks (233 in Jan 2024) outpace RBI's reactivity, though cross-border (Chinese) funding persists. Antara's 2024 task force data reveal 78 promotional content bans, suggesting stronger content moderation than India's social media gaps.

In the Philippines, digital lending frauds 13.4% suspected rate in 2024, per TransUnion rival India's 19%, with Inquirer's November 2025 note of 3,941 cases (down from 7,081) attributing declines to SEC warnings against 28 fake Facebook pages. Scam Watch HQ's 2025 crisis report flags 74% targeting (investments 65%), akin to our urgency-driven lures, while BWorld's November 2025 survey shows more than 60% exposure higher than our 55.1% via shopping scams, but with gendered parallels in Respicio's August 2025 guide on app threats. Philstar's January 2025 projection of $1B market growth underscores inclusion-exploitation paradoxes, yet BSP's real-time mandates (like Clari5's 2025 push) yield faster case drops than India's, highlighting enforcement's role.

Cross-nationally, these frauds thrive on informal digital divides, but variance in regulatory agility (OJK's blocks vs. RBI's penalties) suggests scalable interventions: Regional AI detection consortia could disrupt transnational profiles, adapting RAT's guardians for the Global South.

7. CONCLUSION

This study unveils the alarming scale of fake social media profile-driven instant loan frauds in India, with 55.1% victimization among 432 informal sector workers, predominantly low-income (78.2%) females (60.5%) with limited education (<10th grade: 68.5%). Predatory rates averaged 1,607% p.a., fueled by WhatsApp lures (50%) and escalated via harassment (71.4% shaming, 24.8% nude morphing). Qualitative themes exposed industrialized profile farms, psychological grooming, transnational recovery agents, and profound impacts like suicidal ideation (28%) and family disruptions (35%), underscoring a predatory nexus exploiting digital divides.

The findings extend Routine Activity Theory (RAT) by hybridizing it with technology-enabled predation, introducing a "digital guardian inversion" where AI profiles converge offender routines with vulnerable targets amid absent platform safeguards. Intersectionality illuminates compounded risks for gendered, low-caste informal, enriching victimology and critiquing financial inclusion as a double-edged sword. This framework advances cyber criminology, positing scalable feedback loops for Global South contexts. Longitudinal studies tracking debt trajectories and comparative analyses with Southeast Asian analogs (e.g., Indonesia's Pinjol) could refine interventions. Exploring blockchain for KYC or AI ethics in lending warrants interdisciplinary probes.

8. REFERENCES

1. Agarwal, S., & Singh, R. (2023). Are FinTech lending apps harmful? Evidence from user experience in India. The British Accounting Review, 55(6), Article 101189. https://doi.org/10.1016/j.bar.2023.101189
2. Bossler, A. M., Holt, T. J., & May, D. C. (2011). Predicting online harassment among youth using routine activities theory. Journal of Contemporary Criminal Justice, 28(4), 481–503.
3. https://doi.org/10.1177/1043986211425499
4. Chakraborty, K., & Singh, A. (2025). FLC-Net: Innovative fraud classification in loan applications with federated learning. Machine Learning with Applications, 16, Article 100557.
https://doi.org/10.1016/j.mlwa.2025.100557
5. Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), From crime policy to victim policy (pp. 17–30). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-08152-3_2
6. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608. https://doi.org/10.2307/2094589
7. Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. University of Chicago Legal Forum, 1989(1), 139-167.
8. Creswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications.
9. Deloitte. (2015). Deloitte India banking fraud survey report (Edition II).
https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-deloitte-india-banking-fraud-survey-report-noexp.pdf
10. Gupta, R., & Kumar, S. (2023). Demystifying the misery behind loan apps in India. International Journal of Finance & Banking Studies, 12(1), 1-12. https://doi.org/10.20525/ijfbs.v12i1.2047
11. Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
12. Indian Cybercrime Coordination Centre (I4C). (2025). National cybercrime report 2024. Ministry of Home Affairs, Government of India. https://www.i4c.mha.gov.in/ncrb-reports
13. National Crime Records Bureau (NCRB). (2024). Crime in India 2023. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/crime-in-india
14. National Crime Records Bureau (NCRB). (2025). Cybercrime statistics 2024. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/sites/default/files/CII-2024-Snapshot.pdf
15. Press Information Bureau (PIB). (2025, October 8). Curbing cyber frauds in Digital India. Government of India. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384
16. RBI Working Group on Digital Lending. (2021). Report of the Working Group on digital lending including lending through online platforms and mobile apps. Reserve Bank of India.
https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/DIGITALLENDINGF6A90CA76A9B4B3E84AA0EBD24B307F1.PDF
17. Reserve Bank of India (RBI). (2022). Guidelines on digital lending. RBI/2022-23/95
18. DOR.STR.REC.53/21.04.048/2022-23. https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12303
19. Reserve Bank of India (RBI). (2025a). Digital Lending Directions, 2025.
20. RBI/2025-26/36DOR.STR.REC/21.04.048/2025-26.
https://rbi.org.in/Scripts/NotificationUser.aspx?Id=12848
21. Reserve Bank of India (RBI). (2025b). Annual report 2024-25.
https://www.rbi.org.in/Scripts/AnnualReportPublications.aspx?year=2025
22. Reyns, B. W., Randa, R., & Fisher, B. S. (2016). Victimization patterns and exposures to crime among undergraduate students: A routine activities approach. Criminal Justice Studies, 29(3), 267-285.
https://doi.org/10.1080/1478601X.2016.1209161

23. Sharma, A., & Verma, P. (2025). Predatory loan mobile apps in India: A new form of cyber psychological manipulation. International Journal of Information Management Data Insights, 5(1), Article 100281. https://doi.org/10.1016/j.jjimei.2024.100281
24. Singh, J., & Gupta, M. (2025). Impact of digitization and UPI on small informal businesses in India. Journal of Small Business & Entrepreneurship, 37(4), 1-20. https://doi.org/10.1080/08276331.2025.3919176
25. Supreme Court of India. (2025a). Vishnu vs. State of Kerala (2025 INSC 884). https://api.sci.gov.in/supremecourt/2023/26291/26291_2023_2_1501_62601_Judgement_23-Jul-2025.pdf
26. Supreme Court of India. (2025b). Bank of India vs. Motijhil Branch (2025 INSC 807).
27. https://api.sci.gov.in/supremecourt/2025/1444/1444_2025_3_1503_62154_Judgement_05-Jun-2025.pdf
28. The Reporters' Collective. (2024, February 5). Insurance firms lure bank employees with iPhones, foreign jaunts in fraud scheme. https://www.reporters-collective.in/trc/eng-insurance-fraud
29. The Times of India. (2025, July 18). Loan app scam: HC dismisses accused's bail plea. https://timesofindia.indiatimes.com/city/kochi/loan-app-scam-hc-dismisses-accuseds-bail-plea/articleshow/122769097.cms
30. The Wire. (2025, June 26). Get free credit reports and instant loan access with OneScore. https://thewire.in/ptiprnews/get-free-credit-reports-and-instant-loan-access-with-onescore
31. Trilegal. (2021, December 16). RBI Working Group Report on Digital Lending. https://trilegal.com/wp-content/uploads/2021/12/RBI-Working-Group-Report-on-Digital-Lending.pdf
32. Van Dijk, J. A. G. M. (2006). Digital divide research, achievements and shortcomings. Poetics, 34(4-5), 221-235. https://doi.org/10.1016/j.poetic.2006.05.004
33. Verma, R., & Kumar, A. (2025). Exploring the role of digital financial literacy and personal financial management behavior on financial well-being in urban India. Acta Psychologica, 260, Article 104195. https://doi.org/10.1016/j.actpsy.2025.104195